Claims

1. A method for granting an access to a computer-based object, wherein

- a memory card having a program code processor is provided, with at least one public and one private key assigned to the memory card being stored thereon,
- an item of license information which comprises at least one license code encrypted by means of the public key assigned to the memory card is provided at a computing device controlling the access to the computer-based object,
- a symmetric key which is made available to the memory card and the computing device is generated from a first random number generated by the memory card and from a second random number provided by the computing device,
- the encrypted license code and a specification, provided with a hash value encrypted using the symmetric key, of a function that is to be executed by the memory card for decrypting the license code are transmitted to the memory card,
- the encrypted hash value is decrypted by the memory card and checked for agreement with a hash value computed for the specification of the function to be executed by the memory card,
- if the result of the check is positive, the function for decrypting the license code is executed by the memory card and a decrypted license code is transmitted to the computing device,
- the decrypted license code is provided at least temporarily for accessing the computer-based object.

2. The method as claimed in claim 1,

wherein the public key of the trusted party is provided, protected against manipulations, at the computing device, wherein the license information is digitally signed by means of a private key of the trusted party, and wherein the digital signature of the license information is checked in the computing device with the aid of the public key of the trusted party.

3. The method as claimed in one of the claims 1 or 2, wherein the decrypted license code is provided with a hash value encrypted using the symmetric key, and wherein the encrypted hash value of the decrypted license code is decrypted in the computing device and checked for agreement with a hash value computed for the decrypted license code.

4. The method as claimed in one of the claims 1 to 3, wherein the symmetric key is valid for one access-granting transaction only and is regenerated for each new access request.

5. The method as claimed in one of the claims 1 to 4, wherein

- the license information additionally comprises the public key assigned to the memory card,
- the first random number is transmitted, digitally signed by means of the private key assigned to the memory card, to the computing device,
- the digital signature of the first random number is checked in the computing device with the aid of the public key assigned to the memory card,
- the second random number is transmitted, encrypted by means of the public key of the memory card, to the memory card and decrypted there.

6. The method as claimed in one of the claims 1 to 5, wherein the encrypted license code and the specification, provided with the hash value encrypted using the symmetric key, of the function to be executed by the memory card are transmitted via a secure communications link from the computing device via a reading device to the memory card.

7. The method as claimed in one of the claims 1 to 6, wherein a third random number is generated by the memory card and transmitted to the computing device, wherein a hash value, which is encrypted by means of the symmetric key and the third random number, is computed by the computing device for the specification of the function to be executed by the memory card and transmitted in encrypted form to the memory card, and wherein the hash value encrypted by means of the symmetric key and the third random number is decrypted by the memory card and checked for agreement with a hash value computed for the specification of the function to be executed by the memory card.

8. The method as claimed in claim 7, wherein a fourth random number is generated in the computing device and transmitted to the memory card, wherein a hash value, which is encrypted by means of the symmetric key and the fourth random number, is computed by the memory card for the decrypted license code and transmitted in encrypted form to the computing device, and wherein the hash value encrypted by means of the symmetric key and the fourth random number is decrypted in the computing device and checked for agreement with a hash value computed for the decrypted license code.

9. The method as claimed in one of the claims 1 to 8, wherein the decrypted license code and a check process sequence are aligned with a respective reference specification for granting the access to the computer-based object.

10. A control program which can be loaded into a working memory of a computing device and has at least one code section, upon the execution of which

- the generation of a symmetric key from a first random number generated by a memory card having a program code processor and from a second random number provided by the computing device is initiated,
- the transmission, to the memory card, of a license code encrypted by means of the public key assigned to the memory card and of a specification, provided with a hash value encrypted using the symmetric key, of a function to be executed by the memory card for decryption of the license code is initiated,
- a decryption of the encrypted hash value by the memory card and a check for agreement with a hash value computed for the specification of the function to be executed by the memory card are initiated,
- if the result of the check is positive, an execution of the function for the decryption of the license code by the memory card and a transmission of a decrypted license code to the computing device are initiated,
- the decrypted license code is provided by the computing device at least temporarily for accessing the computer-based object,

when the control program executes in the computing device.